Nonlinear Phenomena in Complex Systems, vol. **17**, no. 3 (2014), pp. 272 - 277

Formalization of Objectives of Grid Systems Resources Protection against Unauthorized Access

M. O. Kalinin* and A. S. Konoplev†
Saint-Petersburg State Polytechnic University,
29 Politechnicheskaya Str, 195251 Saint-Petersburg, RUSSIA
(Received 31 March, 2014)

The paper reviews the problem of security for computing resources and user data in Grid systems. It discusses the security related characteristics of Grid system architecture and provides the threat model. It also considers methods aimed to improve security of Grid systems and highlights their disadvantages. The Grid system specification based on Petri net is proposed which allows modeling job requests distribution in accordance with requirements of security policies and formalization of the objectives of Grid systems protection against unauthorized access.

AMS Subject Classification: 68U35
Keywords: Grid system, information security, access control, model, security policy, Petri net

1. Introduction

Nowadays, Grid systems as type of distributed computing systems have become a leading technology which is used to solve work-intensive and resource-intensive tasks in scientific and commercial areas. Due to a high value of information being processed by Grid hosts, Grid systems are focused on aspects of information security.

Grid system architecture reflects the hierarchical organization of the protocol stack [1], which is based on a set of basic protocols (resource protocols and communication protocols) for different types of computational resources. Its upper level is formed by applications that use resources and communication protocols for cooperation of Grid system users. Implementation of any Grid system includes the following components: computers with graphical user interface, resource providers, core services that are run on separate servers. According to the types of tasks that users can solve on Grid systems, its resources can be classified as:

1. Computing resources. These resources are used to solve time-consuming tasks that require significant amounts of CPU time or memory.

2. Informational resources. These resources are necessary for users of Grid systems, and are stored typically in remote host systems.

3. Software resources. These resources provide to the users availability to use software that is not accessible from their own environment.

4. Network resources. These are used for communication tasks.

Resource sharing mechanism is implemented through virtual organizations (VO), which are dynamic communities of Grid system users, united according to the tasks they solve [2].

2. Grid systems threat model

Grid systems are characterized by decentralized and heterogeneous properties and high state dynamics. It makes difficult to ensure the protection of computing and information resources and to use classical access control models. These security issues are

*E-mail: maxim.kalinin@ibks.ftk.spbstu.ru
†E-mail: artem.konoplev@ibks.ftk.spbstu.ru

particularly relevant to critical information and telecommunication systems built using Grid technology. Consequently, we can highlight the following set of types of attacks on Grid systems (generalized threat model built for Grid systems, is presented in Fig. 1):

- **Denial-of-service attacks** are network attacks on basic Grid system services. They can enforce an authorized component to disconnect from the Grid system. They may also cause Grid system overloads, hindering the work of users and services.

- **Malware distribution** is also important problem, because Grid systems provide legal channels for performing distributed computing.

- **Unauthorized access** to Grid system resources. Can be caused by both authorized users and components of Grid systems and external intruders. The following types of unauthorized access are typical for any Grid system:

  – connection to an unauthorized user or system component (unauthorized is a component whose certificate is not issued by a trusted certification center);

  – attempts to access Grid system user data by the host processes and host environment users;

  – attempts to exceed authorized access by the user, Grid system application or service.

To prevent denial-of-service attacks and malware distribution, Grid systems engage software-hardware components called security managers with installed intrusion detection systems, firewalls and antivirus programs [3]. Security managers are connected with dedicated lines, which broadcast alerts in case of intrusion. Each unit, having received an alert, duplicates it to all resource providers under its control. As a result, all units of the Grid system isolate the problematic unit, from which the threat had come, eliminating the possibility of attacks (Fig. 2).

Consideration of services implemented in the popular Grid environments (Globus Toolkit [4], UNICORE [5], gLite [6], Gridbus [7] and BOINC [8]) suggests that security function is currently limited by authorization and authentication [9]. These security mechanisms are aimed at countering attacks of connection to the system by unauthorized users and components.

Computing platform Grid system is based on a local network of personal computers, rather than on dedicated servers (as implemented in the cloud computing systems). Thus, an important task to protect Grid system user data from unauthorized access is to isolate the specified data from the effects of the host environment. Therefore Grid system units employ a trusted hardware and software platform [10], and help to protect one from the harmful processes and unwanted privileged local users from the host environment.

3. Access control in Grid systems

As a mechanism of user access control, Grid systems implement information security policies that govern access rules in the form of "subject–object–access rights". Compliance with the requirements of information security policy is guaranteed through monitoring and control of user access to data and resources of Grid systems. Heterogeneity of Grid systems, having multiple user authentication mechanisms, and lack of centralized security server make it difficult to implement classical access control models. Paper [11] provides a logical model of access control in Grid systems, which allows to define an information security policy in the Grid system, taking into account different user authentication mechanisms for computing resources access. In that case, a Grid system is represented as a set of states. Each Grid system user may at any time participate in several VOs.

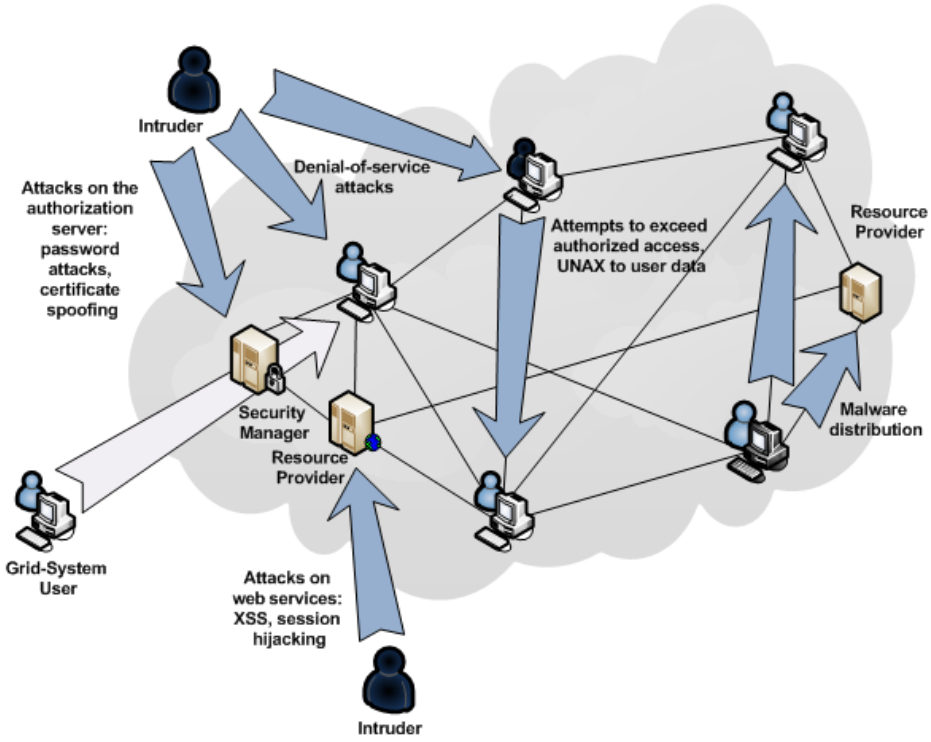

FIG. 1: Generalized Grid system threat model.

Thus, static description of Grid systems security states is not enough to neutralize the threat of attempts to exceed authorized access by users, applications or services in Grid systems. It is necessary to simulate the dynamic distribution of user requests. The authors propose an approach to protect Grid system resources against unauthorized access based on secure distribution of user requests for the provision of computing resources in accordance with the requirements of information security policies. This approach provides the description of predefined relations in the host environment and takes into account the dynamics of Grid system states, using mathematical tools of functional colored Petri nets.

Grid system nodes (resource providers) are represented as finite non-empty set of vertices $M = \{m_i\}$ of Petri net defined by graph $c = (M,\ T,\ *)$ where $T = \{t_i\}$ is a set of transitions between vertices of the graph. Tokens (markers of) colored Petri nets denote Grid system user requests to provide a certain type of resource. Each transition between the vertices of the graph is represented by probability function (for example, the residence time of the label in the queue).

Let us consider the simplest example of a Grid system (see Fig. 4) with a single resource provider M_1 and three host systems. Generally, the set of users U and the set of vertices M may not coincide. This is because several users can operate the same Grid system node. On the other hand, some nodes may have no authorized users, though the computing resources at a given node may be included in the Grid system. On average, let one Grid system user refer to one host system. Let us assume that all user requests pass through resource provider M_1, and only one user U_1 can initiate the task. Yet, the specified task can be always performed by other host systems U_2 and U_3.

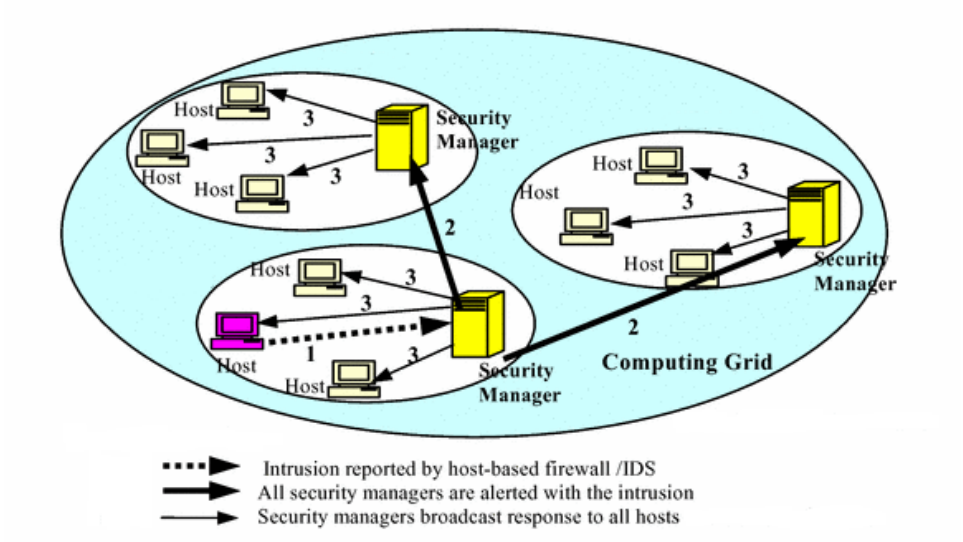

FIG. 2: Network attack countermeasures implemented in Grid systems.

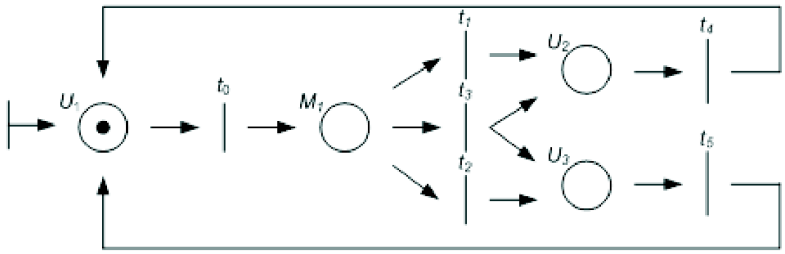

FIG. 3: Example of Grid systems using Petri nets.

Let t_i be a token transition probability from one Grid system node to another. In this example $t_0 = 1$, since the Grid system has only one resource provider, and all user requests pass through that provider. So, t_4 and t_5 are the probabilities, that computational power of units U_2 and U_3 will be needed to perform a user task. t_3 is the probability that the combined computational powers of two host systems for the user task will be needed. Such situation may occur when two programs, each installed in its own host system, are required to fulfil one task. t_4 and t_5 are the probabilities, that the task will be successfully filled on the corresponding host system, with the required result, returned to the user U_1. The initial marking of the Petri net is characterized by a vector $\mu = (\mu(M_1), \ldots, \mu(M_n))$ where n is the number of positions of Petri nets. For Petri net on Fig. 3 vector $\mu = (1, 0, 0, 0)$ is appropriate.

There is, normally, more than one resource provider in real Grid system, with a certain number of users connected to each resource provider (ex. fig. 5). In addition, resource providers are able to redistribute tasks among themselves (transitions t_{31} and t_{32}) in two cases:

1. The resource provider reached the maximum allowed number of active requests. In this case the load balancing between resource providers occurs.

2. Host system, connected to the resource provider, does not have the right type (or quantity) of resources. In this case a subset of queries is transmitted to the other suitable resource provider.

Function transitions between vertices of the graph are defined probabilistically in this Grid system model. It does not take into account limitations imposed by the requirements of information security policies. We turn to the functional Petri nets, defining the form of function, acting on the set of transitions $\{t_{ij}\}$, so that when one moves tokens from one graph vertex to another, conformance with the given constraints is being checked. Consider the set of *Rights* (constraints), specified in the requirements of information security policy, as well as a set of predefined *Relations*, namely a set of queries (Petri net token), which are currently present in the specified Grid system node. Let us set a token type $T = \langle F,\ A\rangle$ where F is a class of resources, requested by a Grid system user (computing resources, user data, etc.) and A are security attributes that are used to verify compliance with information security policies.

For example, Fig. 4 shows the tokens, corresponding to requests for providing resources of two classes, on the tops of the U_1 and U_4, respectively. Security attributes are the user IDs, which initiated the request: $U \subseteq A$. Applied to the vertices of the graph c, a tuple T determines the type of the Grid system computing node.

Moving the user's task from node m_i to node m_j means the fulfillment of sufficient conditions for t_{ij} transition firing. We introduce an operator Ψ which acts on the set of transitions $\{t_{ij}\}$:
Ψ: $\langle U,\ M,\ Rights,\ Relations\rangle \to$ {TRUE, FALSE}.

Parameters that define the domain of specified operator are variables. Formalization of the operator, as well as the presence or absence of these parameters in the range of the operator, allows us to define a set of *application tasks, designed to protect resources of Grid systems from unauthorized access*:

1. **The task of user requests secure distribution**. Given sets *U, M, Rights, Relations*. The presence of these parameters allows us to build an algorithm for finding host systems for query execution set by the user, taking into account the requirements of information security policies. Thus, a prerequisite secure distribution of user requests for the provision of computational resources of Grid systems is performed where each state of the system meets the requirements of information security policy.

2. **The task of information security policy requirements verification**. *U, M, Rights* are given sets and the range of Ψ operator is known. These parameters allow us to solve the problem of identifying the predefined relationships that lead to deviations from the requirements of information security policies.

3. **The task of Grid systems secure configuration**. *U, M, Rights* are given sets and the range of Ψ operator is known. These parameters allow us to create a description for a safe Grid system condition, which can then be used to automate the process of setting up Grid systems in compliance with information security policies.

4. **The task of identifying violators of security**. *M, Rights* and *Relations* are given sets. These parameters provide the identification of the subjects of access (Grid system users), performing actions, violating the requirements of information security policies.

4. Conclusion

Grid system special service, operating on the resource provider, performs hosts searching, suitable for user tasks execution. Therefore, to solve these problems, the Ψ operator must be integrated into a specified service. Thus, when choosing a suitable node, not only the availability and the type of Grid system resources at the disposal of the host ware taken into account but also requirements of information security policy, permitting or prohibiting the use of resources

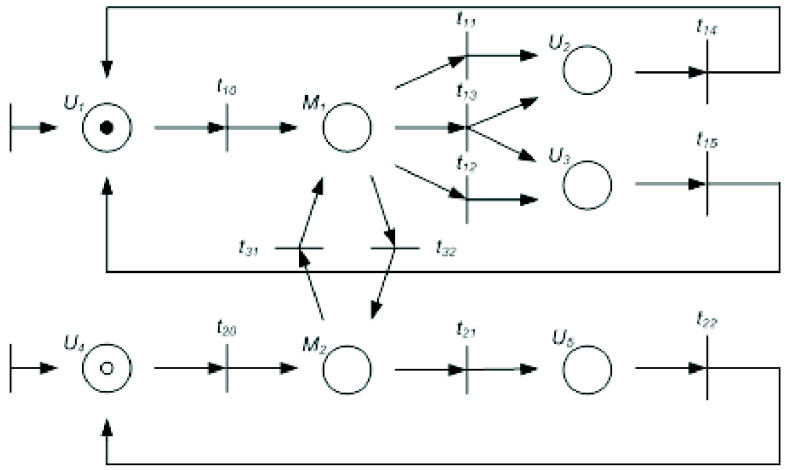

FIG. 4: Types of Grid system resources and computing nodes (example with two resource providers).

on the specified system node for the user, who initiated the request.

Formal solution of the specified tasks and software module implementation as a part of resource provider will automate the safety analysis process and provide a high level of reliability and security of Grid systems.

References

[1] I. Foster, C. Kesselman. *The Grid: Blueprint for a New Computing Infrastructure.* (2nd Edition). (Morgan Kaufmann, 2004).

[2] The Globus Security Team. Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective. Internet resource: *globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf.*

[3] Internet resource:*www.unicore.eu.*

[4] A. Sciaba, S. Burke, S. Campana, E. Lanciotti, M. Litmaath, P. M. Lorenzo, V. Miccio, C. Nater, R. Santinelli. Glite 3.2 User Guide. (CERN, 2011).

[5] R. Buyya, S. Venugopal. The Gridbus Toolkit for Service Oriented Grid and Utility Computing: An Overview and Status Report. In: *Procedings of 1st IEEE international workshop on Grid Economics and Business Models,* Seoul, Korea, April 23, 2004. (IEEE, 2004).

[6] Internet resource:*boinc.berkeley.edu*

[7] M.O. Kalinin, A.S. Konoplev, I.A. Markov. Monitoring the implementation of information security policies in grid-systems. In: *Proceedings of "Information Security of Russian Regions (ISRR-2011)".* (SPOISU, St. Petersburg, 2011).

[8] R. Alfieri, R. Cecchini, V. Ciaschini, L. Dell'Agnello, A. Frohner, A. Gianoli, K. Lorentey, F. Spataro. *VOMS, an Authorization System for Virtual Organizations.* Lecture Notes in Computer Science. (Springer, 2003).

[9] Shanshan Song, Kai Hwang, Mikin Macwan. *Fuzzy Trust Integration for Security Enforcement in Grid Computing.* (Springer, 2004).

[10] H. Lohr, H. V. Ramasamy, A. Sadeghi, S. Schulz, M. Schunter, C. Stuble. *Enhancing Grid Security Using Trusted Virtualization.* Lecture Notes in Computer Science. (Springer, 2007).

[11] M.O. Kalinin, I.A. Markov. Verification of Security Policies Requirements In Grid-Systems. Information Security Problems. Computer Systems. No. 2, 9 (2011).